TraderTraitor: Deep Dive

By Merav Bar

Published: 2025-07-28 · Archived: 2026-04-05 19:50:16 UTC

TraderTraitor is a cluster of North Korean activity aimed at stealing digital assets (cryptocurrencies such as Bitcoin and Ether). In addition to leveraging traditional techniques such as sending phishing emails and infecting victims with trojanized software, TraderTraitor has conducted more complex operations including supply chain compromises and diverting legitimate transactions. Since its first public mention in 2022, TraderTraitor has been linked to major cryptocurrency thefts and has targeted cloud services and software development platforms in operations like the JumpCloud supply chain attack and the ByBit hack. Given the nature of this actor's current activities and the threat they pose to cloud customers globally, Wiz Threat Research has decided to publish this deep-dive into their history and tradecraft.

Who is TraderTraitor?

"TraderTraitor" was originally a codename used by the U.S. government to describe a cluster of North Korean state-sponsored cyber activity. In an April 2022 joint advisory, the FBI, CISA, and U.S. Treasury confirmed that the DPRK-backed entities behind TraderTraitor are tracked as Lazarus Group, APT38, BlueNoroff, and Stardust Chollima. These names refer to North Korea's elite hacking units, and the TraderTraitor activity appears to be part of their financially-motivated operations. TraderTraitor has also been assigned UNC4899 [GTIG], Jade Sleet [MSTIC] and Slow Pisces [Unit42].

Multiple government and industry reports since 2022 have attributed major cryptocurrency thefts to TraderTraitor, while underscoring its Lazarus lineage. For example, the FBI and Japan's NPA attributed a $308 million Bitcoin DMM exchange heist (May 2024) to TraderTraitor, calling it a Lazarus subgroup characterized by using simultaneous social engineering of multiple employees to gain initial access to their target. Similarly, a $1.5 billion hack of the Bybit crypto exchange in late 2024 was attributed by the FBI to "North Korean TraderTraitor actors". These attributions cement TraderTraitor as an operation under the Lazarus umbrella. North Korea's Reconnaissance General Bureau (RGB) is believed to be the sponsoring agency behind Lazarus and its subgroups like TraderTraitor, with some analysis pointing specifically to the 3rd bureau (Bureau of Foreign Intelligence).

Financial gain is the primary strategic objective of TraderTraitor. North Korea's regime, under heavy sanctions, leverages these cyber operations to steal cryptocurrency and generate revenue to fund state programs. The TraderTraitor campaigns specifically target blockchain and cryptocurrency organizations – such as exchanges, DeFi platforms, crypto startups, venture funds, and even wealthy individual crypto holders – with the goal of stealing digital assets. Stolen funds (often in the form of Bitcoin, Ether, or other crypto) are laundered and converted to support North Korea's priorities. This exclusive focus on blockchain targets and its use of supply chain attacks using trojanized open-source packages (npm, PyPI) differentiates them from other Lazarus sub-groups.

Beyond direct theft, TraderTraitor may also pursue strategic espionage objectives in the crypto/blockchain sector. Reports indicate the attackers seem to seek to acquire sensitive cryptocurrency intellectual property and technology. However, the immediate operational goal is typically theft rather than long-term espionage: TraderTraitor intrusions often move quickly from initial access to illicit blockchain transactions within days. This aligns with Lazarus's dual goals for espionage and profit: TraderTraitor campaigns join nation-state tactics with financially driven outcomes, effectively turning cybercrime into a revenue stream for the North Korean state.

Evolution of TraderTraitor

TraderTraitor has conducted several major campaigns since 2020, all sharing common tactics (social engineering, trojanized malware or code) but targeting different parts of the cryptocurrency ecosystem.

Trojanized Cryptocurrency Applications (2020–2022)

The earliest campaign attributed later to TraderTraitor involved trojanized cryptocurrency trading applications delivered to victims under the pretense of job recruitment. According to a U.S. government advisory, the attackers send phishing messages [T1566.003] on platforms like LinkedIn, Slack, or Telegram to employees of crypto companies (especially those in DevOps, IT, or system admin roles). These messages posed as recruiters offering lucrative jobs and enticed targets to download fake crypto applications [T1204.002] that contain malicious payloads. These malicious apps – built on JavaScript [T1059.007] and Node.js using the Electron framework – are referred to collectively as "TraderTraitor" apps by U.S. authorities.

The initial apps themselves appeared to be functional (e.g. crypto price trackers or trading tools) and even feature polished websites and valid code signatures to appear legitimate, but in reality, they are repurposed open-source crypto tools implanted with malicious update routines. These apps were often digitally signed with compromised or fraudulent Apple code-signing certificates (later revoked) to bypass security warnings [T1553.002].

Each malicious application had an "update" mechanism that would contact a hardcoded C2 URL [T1105]. The C2 server could respond with an encrypted second stage payload (using AES-256 [T1027]) that the app would decrypt and execute on the victim's machine. In this way, TraderTraitor apps delivered malware such as MANUSCRYPT (a remote access trojan) onto victims' systems. MANUSCRYPT would then harvest system info [T1082], execute arbitrary commands [T1059], and ultimately seek out cryptocurrency wallet keys or credentials to enable theft of funds.

This campaign, active through 2020–2022, successfully breached multiple organizations. For instance, Lazarus used similar AppleJeus malware-laced apps in earlier operations to infiltrate crypto exchanges. By mid-2022, TraderTraitor's trojan apps were implicated in major thefts, such as the Ronin Network (Axie Infinity) breach where Lazarus stole $620 million after compromising a blockchain game company employee via a fake job offer PDF [T1566.001] and application (this incident pre-dated the TraderTraitor codename but demonstrates the same tactics). The confirmed impact of these campaigns includes numerous corporate network intrusions and cryptocurrency thefts, though specific victim names are often undisclosed.

Supply Chain Compromises (2023)

In 2023, TraderTraitor expanded into open-source software supply chain attacks, marking one of the first known cases of a nation-state APT leveraging public package repositories for attacks. In a campaign uncovered in early 2023, the threat actors impersonated software developers and engaged targeted engineers in collaborative projects on GitHub. After establishing trust (often via LinkedIn or other social contact), the TraderTraitor operators invited the victims to collaborate on a GitHub repository that contained malicious JavaScript packages sourced from npm as dependencies [T1195.001].

This operation primarily targeted developers working at blockchain and fintech firms. By compromising a developer's machine or injecting code into a project, the attackers aimed to infiltrate the victim company's software supply chain. The end goal would be either to directly steal crypto (if the developer had wallet access) or to trojanize the company's software updates in order to infect many downstream systems.

GitHub and security researchers (e.g. Phylum, Checkmarx) identified this campaign in 2023. GitHub confirmed the threat actor's identity as North Korea's Jade Sleet/TraderTraitor and took action by suspending the malicious npm accounts and repositories. Several malicious domains tied to this NPM campaign were identified, masquerading as legit package or crypto services.

JumpCloud compromise

Another significant supply chain-related attack occurred in July 2023 and targeted a cloud service provider, JumpCloud. In that case, TraderTraitor (UNC4899) compromised JumpCloud's platform via spear-phishing, then abused JumpCloud's privileged access to push a malicious update [T1195.002] to a handful of cryptocurrency industry customers [T1199]. JumpCloud, a cloud identity management (SaaS) provider, revealed that fewer than five customers were impacted by this breach. Mandiant's investigation of one victim confirmed the intrusion stemmed from the JumpCloud compromise and attributed it to TraderTraitor. The JumpCloud incident is a rare example of cloud supply-chain compromise in which the attackers leverage a vendor's infrastructure (in this case, identity management) to bypass traditional defenses.

Analysis of the JumpCloud compromise

Fake Job Lures and Crypto Exchange Heists (2024–2025)

One of the staples of North Korean social engineering has been "Operation Dream Job"-style attacks, so named for their use of a fake job offer as a lure. TraderTraitor's particular take on this technique has been the use of bogus coding challenges for developers working at crypto exchanges, often delivered as PDF attachments and links to GitHub repositories. They then leverage this foothold in the victim organization in order to pivot to crypto transaction systems, ultimately stealing huge sums of digital currency.

While TraderTratior isn't the only North Korean actor to target this sector (WazirX, an Indian crypto exchange, was compromised in July 2024 by a North Korean actor using similar techniques to those of TraderTraitor), they have certainly had the most public success in terms of raw numbers.

The attack on Ginco and DMM bitcoin (4502.9 BTC or 308 million USD)

In March 2024, a TraderTraitor operative posed as a recruiter and lured a developer at Ginco into running a malicious Python script from a fake coding challenge hosted on GitHub [T1059.006,T1204.002]. The malware, identified as RN Loader and RN Stealer, harvested sensitive data including SSH keys, saved credentials, and cloud configurations [T1552.004]. Using the stolen session cookies [T1550.004], the attackers accessed Ginco's internal systems and breached an unencrypted communication channel linked to DMM Bitcoin. By late May, they exploited this access to divert 4,502.9 BTC (approximately $308 million) in a fraudulent transaction. The FBI and Japanese authorities formally attributed the attack to TraderTraitor.

The Bybit hack

Another massive heist followed in late 2024: the Bybit exchange hack, in which TraderTraitor successfully stole over 400,000 ETH and staked ETH—amounting to approximately $1.5 billion USD. While details of the initial intrusion were not fully public at the time, subsequent investigation revealed that the operation was both sophisticated and emblematic of TraderTraitor's evolving tradecraft. In early February 2025, the attacker set up infrastructure by registering the domain getstockprice[.]com, which was later used as a command-and-control (C2) endpoint. Shortly after, a developer's macOS workstation—Developer1—was compromised via a malicious Python application likely delivered through social engineering on Telegram or Discord.

This application included a malicious docker image [T1609] and contacted the attacker's domain. The attacker then used stolen AWS session tokens to access Safe{Wallet}'s cloud environment and attempted to register a virtual MFA device to maintain persistence. Throughout mid-February, the attacker conducted reconnaissance, enumerating IAM roles, S3 buckets, and other cloud assets [T1580]. By late February, they had moved to active C2 communication and tampered with Safe{Wallet}'s statically hosted frontend (built with Next.js) by injecting malicious JavaScript [T1578.005]. This payload was designed to detect Bybit transactions and modify them in real time, redirecting funds to the attacker's wallet. The exploit was executed later that month, and the script was scrubbed from the site shortly after - finalizing the theft.

The FBI publicly attributed the incident to TraderTraitor in January 2025, confirming the operation leveraged Safe{Wallet} as a supply chain weak point rather than compromising Bybit infrastructure directly. This marked one of the largest cryptocurrency thefts ever, and further underscored TraderTraitor's ability to combine cloud access, social engineering, and web app tampering to devastating effect.

Analysis of the Bybit compromise

A Focus on Cloud

TraderTraitor has demonstrated a sustained interest in cloud-centric and cloud-adjacent attack surfaces, often with a final goal of compromising companies that are customers of cloud platforms rather than the platforms themselves. This was evident in the JumpCloud breach, where the group infiltrated a cloud-based identity and device management provider to compromise downstream organizations. A similar pattern emerged in the Bybit heist, where TraderTraitor gained access to Safe{Wallet}'s AWS environment by stealing active session tokens from a compromised developer machine—effectively bypassing multi-factor authentication. The attackers leveraged these credentials to conduct reconnaissance, plant malware in S3 buckets, and explore IAM roles and

cloud asset configurations before injecting malicious JavaScript into a web application frontend to redirect crypto transactions.

Their ability to abuse trusted cloud service providers as supply chain pivots—for example, by injecting malicious code into an orchestration framework—highlights their capabilities in cloud-native compromise paths, even if these are not their main focus. Moreover, their malware has evolved to exfiltrate cloud service credentials and configuration files [T1552.004] from infected developer machines, as seen with RN Stealer. These tactics suggest that TraderTraitor understands the value of cloud credentials, APIs, and SaaS integrations as a route to privileged access and broader lateral movement [T1087.004]. Their adoption of open-source package poisoning and GitHub-based lures further supports their intent to penetrate cloud-connected development pipelines, making cloud environments a high-value vector in their ongoing operations.

How can Wiz help?

Prevention

1. Wiz customers can implement Controls for network and identity segmentation to obstruct potential lateral movement to highly privileged principals or sensitive resources, limiting the blast radius of potential employee workstation compromise.
2. Wiz customers can identify overly permissive users in order to limit developer permissions to the minimum required set, which is especially important in production and CI/CD environments.
3. Wiz customers can rely on Wiz CSPM, Secrets Scanner, and Dynamic Scanner to monitor cloud configuration and secrets (e.g., AWS credentials, SSH keys) for anomalies or inadvertent exposure.
4. Wiz Code customers can track code dependencies to detect suspicious packages, and use Cloud-to-Code mapping to identify what cloud resources these packages may have built.

Detection

1. Wiz Defend customers can monitor for enumeration attempts, cloud key compromise, suspicious MFA device registration, and many other techniques employed by TraderTraitor.
2. Wiz Sensor customers can investigate any outgoing connections to campaign-associated IP addresses, and Wiz Defend customers can further investigate by querying for events initiated by principals connecting from IP addresses linked to this campaign.
3. Wiz customers can use the Security Graph and Wiz Sensor to detect malware matching related indicators of compromise in their environment.

   Screenshot from Wiz Threat Actors page for TraderTraitor

Summary

TraderTraitor is a financially motivated North Korean threat subgroup of Lazarus, targeting the cryptocurrency and blockchain ecosystem since at least 2020. Their operations blend nation-state sophistication with cybercriminal tactics, relying heavily on social engineering, trojanized applications, and supply chain compromises to steal digital assets. Publicly attributed by organisations like the FBI and Japan's NPA, the group has been linked to some of the largest crypto heists to date, including attacks on DMM Bitcoin and Bybit. TraderTraitor has also expanded into cloud-adjacent attacks—compromising vendors like JumpCloud—and actively targets developers through poisoned open-source packages and GitHub lures. Their evolving methods underscore the risk they pose to cloud-connected organizations.

TTPs

All Mitre ATT&CK techniques are also detailed in this map.

MITRE Tactic	Technique & ID	TraderTraitor Example
Initial Access	Spearphishing Link/Attachment (T1566.002)	LinkedIn recruiter sends target a malicious app or GitHub link.
Initial Access	Spearphishing via Service (T1566.003)	Malicious messages delivered through Slack, LinkedIn, Telegram.
Initial Access	Spearphishing with Attachment (T1566.001)	Fake PDF job offers deliver malware.
Execution	User Execution (T1204.002)	Victim runs trojanized crypto app or installs malicious NPM package, executing malware.
Execution	Command and Scripting Interpreter: JavaScript (T1059.007)	TraderTraitor apps use JavaScript and Node.js.
Execution	Command and Scripting Interpreter: Python (T1059.006)	Fake coding challenges delivered as Python scripts.
Execution	Command and Scripting Interpreter (T1059)	Malware executes arbitrary commands on host.
Persistence	Valid Accounts (T1078)	Stolen credentials (cookies, keys) used to maintain access as a legitimate user.
Defense Evasion	Subvert Trust Controls: Code Signing (T1553.002)	Malware apps signed with stolen or fake Apple Developer certs.
Defense Evasion	Acquire Code Signing Certificate (T1588.003)	Threat actor obtains or uses compromised certs to sign apps.

MITRE Tactic	Technique & ID	TraderTraitor Example
Credential Access	Unsecured Credentials: Credentials In Files (T1552.004)	RN Stealer extracts credentials and cloud configs from files.
Credential Access	Credentials from Password Stores (T1555)	Steals saved passwords, SSH keys, cloud service credentials.
Lateral Movement	Use Alternate Authentication Material (T1550.004)	Session cookies used to impersonate users and pivot internally.
Collection	System Information Discovery (T1082)	Manuscrypt collects host details to support further exploitation.
Command & Control	Ingress Tool Transfer (T1105)	Malware retrieves second-stage payloads from attacker C2.
Command & Control	Application Layer Protocol: Web Protocols (T1071.001)	Malware uses HTTPS callbacks to C2 servers.
Command & Control	Obfuscated Files or Information (T1027)	AES-256 encryption used to conceal payloads.
Exfiltration	Exfiltration Over C2 Channel (T1041)	Sensitive data (e.g. keys, credentials) exfiltrated via HTTPS.
Impact	Data Manipulation / Cryptocurrency Theft	Initiates unauthorized blockchain transactions.
Resource Development	Compromise Software Dependencies and Development Tools (T1195.001)	Malicious NPM/PyPI packages used to compromise dev environments. Split JavaScript malware in npm packages, first-stage downloader and second-stage loader.
Resource Development	Compromise Infrastructure: Software Supply Chain (T1195.002)	JumpCloud supply chain attack to access downstream crypto firms.
Discovery	Account Discovery: Cloud Account (T1087.004)	Identifies cloud environments and configurations for lateral movement.
Lateral Movement	Trusted Relationship (T1199)	Uses compromised cloud service provider to reach customer networks.
Initial Access	Container Images (T1609)	Use of a malicious Docker image to initiate execution.

MITRE Tactic	Technique & ID	TraderTraitor Example
Persistence	Create or Modify System Process: Cloud Service Modification (T1543.003)	Attempt to register a virtual MFA device to persist access.
Discovery	Cloud Infrastructure Discovery (T1580)	Enumeration of IAM roles, S3 buckets, and other cloud assets.
Defense Evasion	Modify Cloud Compute Infrastructure (T1578.005)	Injection of malicious JavaScript into statically hosted frontend (Next.js app).

Tools

Type	Value/Name	Description
Malware	RN Loader	First-stage loader used to collect basic system info and connect to C2.
Malware	RN Stealer	Python-based infostealer targeting SSH keys, saved logins, and cloud service credentials.
Malware	GopherGrabber	Go-based stealer/backdoor with credential theft and C2 via RC4/MD5.
Malware	GolangGhost	Go-based cross-platform RAT used in ClickFix campaign.
Malware	ThreatNeedle	Lazarus RAT used in espionage, reused by TraderTraitor in South Korea.
Malware	AGAMEMNON	Backdoor used in updated TraderTraitor campaigns.
Malware	wAgent	Known Lazarus backdoor reused in TraderTraitor activity.
Malware	SIGNBT	Lazarus malware family reused in updated TraderTraitor operations.
Malware	COPPERHEDGE	RAT associated with Lazarus, observed in TraderTraitor activity.
Malware	TIEDYE	Custom backdoor targeting macOS, heavily obfuscated to prevent detection.
Package	pycryptoenv / pycryptoconf	Typosquatted Python packages targeting crypto developers via PyPI.
Infrastructure	GitHub repos / fake interview pages	Used to deliver malware like GopherGrabber and GolangGhost.

Type	Value/Name	Description
Infrastructure	Fake Willo video interview platform	Used to deliver malware post-interview engagement.
Software Exploit	Innorix Agent flaw	Used for lateral movement within Korean networks.

Indicators of compromise from the campaigns listed above can be found in the Wiz Threat Research public IOC database.

References

- Checkmarx blogpost
- Javier Calderon Jr (xthemadgenius) blogpost
- S2W report
- Sekoia blogpost
- HivePro advisory
- GTI blogpost
- JPCert advisory
- CISA advisory
- Broadcom blogpost
- Wired article
- SentinelOne blogpost
- Github blogpost
- Unit42 blogpost
- Elliptic blogpost
- Phylum blogpost 1
- Phylum blogpost 2
- ReversingLabs blogpost
- Kaspersky blogpost
- Elastic blogpost

Source: https://www.wiz.io/blog/north-korean-tradertraitor-crypto-heist